PEREGRINE REAL-TIME HYPERVISOR

The Peregrine Real-Time Hypervisor was developed with a strong focus on security. Peregrine provides strong isolation between workloads, both in terms of security and safety. Workloads can be bare-metal applications, real-time or regular operating systems, containers and more. Security has been built into the design from the ground up, with the principles of minimal rights assignment and workload isolation consistently implemented. A secure boot process protects against unauthorized access right from system startup. With only 18,000 lines of code that rely on hardware and software defense mechanisms throughout - such as guaranteed integrity of the program control flow, support for Arm Pointer Authentication (PAC) and Branch Target Instructions (BTI), a shadow stack and stack canaries - the Peregrine hypervisor sets new standards in terms of embedded security. In addition, security is guaranteed by continuous integration tests, unit tests, runtime self-tests, static analyses, and fuzzing.

At the heart of our hypervisor is a real-time scheduler that grants critical tasks exclusive access to resources, ensuring the performance of critical system components. The hypervisor impresses with a boot time overhead of less than 300 milliseconds in typical scenarios and a low runtime performance impact, which is less than 2% for typical workloads such as Linux and negligible with exclusive resource allocation. Peregrine also enables efficient inter-VM communication and supports either the exclusive allocation of resources or the shared use of devices between VMs via virtio.

The compatibility of the Peregrine hypervisor extends across a wide range of workloads - from bare-metal applications, unikernels and containers to real-time operating systems or extensive operating systems. No changes to existing workloads are required to combine them with Peregrine. The hypervisor can be integrated directly into existing build processes, with configuration information being provided via a manifest file. This includes information on VMs, authorizations and device access. Finally, Peregrine offers robust over-the-air upgrade capabilities with extensive recovery options designed for the space. With these features, the Peregrine Real-Time Hypervisor sets new standards for security, performance, and reliability in real-time systems. The basic functionalities of the Peregrine hypervisor are made available open source on the Github platform.[1]

SYSTEM REQUIREMENTS

- Supported platforms: Armv8-A (x86 planned)
- 4 GB RAM or more recommended for multiple VMs
- SMMU/IOMMU optional for peripheral access protection
- Memory footprint: Hypervisor binary has a size of only 140kB

[1] https://github.com/SANCTUARY-Systems/Peregrine-Hypervisor